F ENT COOPERATION TREA

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 07 May 2001 (07.05.01)	
International application No. PCT/EP00/06510	**Applicant's or agent's file reference** P99026WO.1P
International filing date (day/month/year) 10 July 2000 (10.07.00)	**Priority date** (day/month/year) 12 August 1999 (12.08.99)
Applicant MARTIN, Tobias et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

24 January 2001 (24.01.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Athina Nickitas-Etienne

Telephone No.: (41-22) 338.83.38

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts P99026WO.1P	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/EP 00/ 06510	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 10/07/2000	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)* 12/08/1999
Anmelder DEUTSCHE TELEKOM AG		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. _____

   [ ] wie vom Anmelder vorgeschlagen

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

   [X] keine der Abb.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/06510

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, INSPEC, PAJ, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	LENNON R E ET AL: "Cryptographic key distribution using composite keys" BIRMINGHAM,ALABAMA, DEC.3-6, 1978,NEW YORK, I.E.E.E,US, Bd. CONF. 1978, 3. Dezember 1978 (1978-12-03), Seiten 26101-26116-6, XP002098158 Seite 26.1.4, linke Spalte, Zeile 23 -Seite 26.1.5, rechte Spalte, Zeile 8 Seite 26.1.6, linke Spalte, Zeile 14 - Zeile 17 ---	1
Y	MENEZES ET AL.: "HANDBOOK OF APPLIED CRYPTOGRAPHY" 1997 , CRC PRESS , BOCA RATON (US) XP002152150 Seite 528, Zeile 22 - Zeile 24 ---	1

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
7. November 2000	22/11/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/06510

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7. April 1993 (1993-04-07) Seite 9, Zeile 10 - Zeile 23 ---	1
A	BURMESTER M ET AL: "SECURE AND EFFICIENT CONFERENCE KEY DISTRIBUTION SYSTEM" ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES,SPRINGER VERLAG,DE, 1995, Seiten 275-286, XP000934269 in der Anmeldung erwähnt Seite 279, Absatz 3.3 -----	1

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 00/06510

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP 0535863 A	07-04-1993	US	5241599 A	31-08-1993
		AU	648433 B	21-04-1994
		AU	2351392 A	08-04-1993
		CA	2076252 A,C	03-04-1993
		JP	2599871 B	16-04-1997
		JP	6169306 A	14-06-1994
		NO	923740 A	05-04-1993

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. Februar 2001 (22.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/13567 A1

(51) Internationale Patentklassifikation[7]: H04L 9/08

(21) Internationales Aktenzeichen: PCT/EP00/06510

(22) Internationales Anmeldedatum:
10. Juli 2000 (10.07.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 38 198.4 12. August 1999 (12.08.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **MARTIN, Tobias** [DE/DE]; Spitzengärten 1, D-35466 Rabenau (DE). **SCHAFFELHOFER, Ralf** [DE/DE]; Wittmannstr. 39, D-64285 Darmstadt (DE). **SCHWENK, Jörg** [DE/DE]; Südwestring 27, D-64807 Dieburg (DE).

(74) Gemeinsamer Vertreter: **DEUTSCHE TELEKOM AG**; Rechtsabteilung (Patente) PA1, D-64307 Darmstadt (DE).

(81) Bestimmungsstaaten *(national)*: AU, CA, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) Title: METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS

(54) Bezeichnung: VERFAHREN ZUM ETABLIEREN EINES GEMEINSAMEN SCHLÜSSELS FÜR EINE GRUPPE VON MINDESTENS DREI TEILNEHMERN

(57) Abstract: The inventive method is based on a publicly known mathematical number group (G) and a higher order element of the group $g \in G$. In the first work step, a message corresponding to Ni: $= g^{zi} \bmod p$) is sent by each subscriber (Ti) to all other subscribers (Tj), (zi) being a random number chosen from the set (1, ..., p-2) by a random number generator. In the second work step, each subscriber (Ti) selects a transmission key kij: $= (g^{zj})^{zi}$ for each other subscriber (Tj) from the received message (g^{zj}), with $i \neq j$, for transmitting their random number (zi) to the subscribers (Tj). In the third work step, the common key k is calculated as k: = f(z1, z2, ..., zn) for each subscriber Ti. The inventive method can be advantageously used for generating a cryptographic key for a group of at least three subscribers.

(57) Zusammenfassung: Das erfindungsgemässe Verfahren basiert auf einer öffentlich bekannten mathematischen Zahlengruppe (G) und einem Element der Gruppe $g \in G$ grosser Ordnung. Im ersten Arbeitsschritt wird von jedem Teilnehmer (Ti) eine Nachricht der Form Ni: $= g^{zi} \bmod p$) an alle anderen Teilnehmer (Tj) gesendet, wobei (zi) eine mittels eines Zufallsgenerators gewählte zufällige Zahl aus der Menge (1, ..., p-2) ist. Im zweiten Arbeitsschritt wählt jeder Teilnehmer (Ti) für jeden weiteren Teilnehmer (Tj) mit $i \neq j$ aus der empfangenen Nachricht (g^{zj}) einen Übertragungsschlüssel kij: $= (g^{zj})^{zi}$ für die Übertragung seiner Zufallszahl (zi) an die Teilnehmer (Tj). Im dritten Arbeitsschritt wird bei jedem Teilnehmer Ti der gemeinsame Schlüssel k als k: = f(z1, z2, ..., zn) berechnet. Das erfindungsgemässe Verfahren lässt sich vorteilhaft zur Erzeugung eines kryptographischen Schlüssels für eine Gruppe von mindestens drei Teilnehmern einsetzen.

WO 01/13567 A1

Verfahren zum Etablieren eines gemeinsamen Schlüssels für eine Gruppe von mindestens drei Teilnehmern

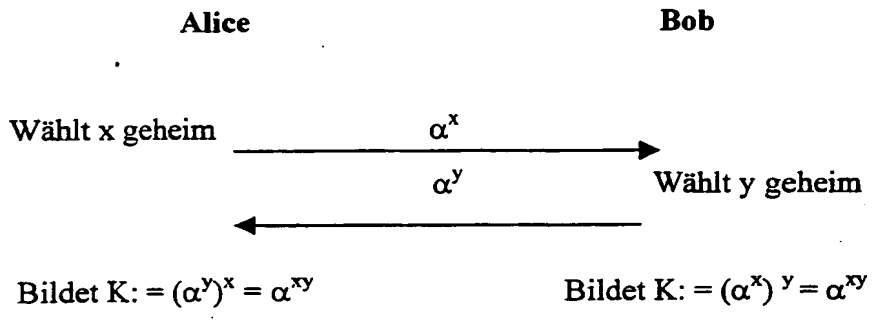
Beschreibung

Die Erfindung betrifft ein Verfahren zum Etablieren eines gemeinsamen Schlüssels innerhalb einer Gruppe von Teilnehmern gemäß dem Oberbegriff des unabhängigen Anspruchs.

Verschlüsselungsverfahren in vielfältiger Art gehören zum Stand der Technik und haben zunehmend kommerzielle Bedeutung. Sie werden dazu eingesetzt, Nachrichten über allgemein zugängliche Übertragungsmedien zu übertragen, wobei aber nur die Besitzer eines Krypto-Schlüssels diese Nachrichten im Klartext lesen können.

Ein bekanntes Verfahren zur Etablierung eines gemeinsamen Schlüssels über unsichere Kommunikationskanäle ist z. B. das Verfahren von W. Diffie und W. Hellmann (siehe DH-Verfahren W. Diffie und M. Hellmann, siehe New Directions in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, November 1976).

Grundlage des Diffie Hellmann Schlüsselaustausches (DH-Schlüsselaustausch) ist die Tatsache, daß es praktisch unmöglich ist, Logarithmen modulo einer großen Primzahl p zu berechnen. Dies machen sich Alice und Bob in dem unten abgebildeten Beispiel zunutze, indem sie jeweils eine Zahl x bzw. y kleiner als p (und teilerfremd zu p-1) geheim wählen. Dann senden sie sich (nacheinander oder gleichzeitig) die x-te (bzw. y-te) Potenz modulo p einer öffentlich bekannten Zahl α zu. Aus den empfangenen Potenzen können sie durch erneutes Potenzieren modulo p mit x bzw. y einen gemeinsamen Schlüssel $K: = \alpha^{xy} \bmod p$ berechnen. Ein Angreifer, der nur $\alpha^x \bmod p$ und $\alpha^y \bmod p$ sieht, kann daraus K nicht berechnen. (Die einzige heute bekannte Methode dazu bestünde darin, zunächst den Logarithmus z. B. von α^x zur Basis α modulo p zu berechnen, und dann α^y damit zu potenzieren.)



Beispiel für Diffie-Hellmann-Schlüsselaustausch

Das Problem beim DH-Schlüsselaustausch besteht darin, daß Alice nicht weiß, ob sie tatsächlich mit Bob kommuniziert, oder mit einem Betrüger. In den IPSec-Standards der Internet Engineering Task Force (IETF RFC 2412: The OAKLEY Key Determination Protocol) wird dieses Problem durch den Einsatz von Public-Key-Zertifikaten gelöst, in denen durch eine vertrauenswürdige Instanz die Identität eines Teilnehmers mit einem öffentlichen Schlüssel verknüpft wird. Dadurch wird die Identität eines Gesprächspartners überprüfbar.

Der DH-Schlüsselaustausch kann auch mit anderen mathematischen Strukturen realisiert werden, z. B. mit endlichen Körpern GF (2^n) oder Elliptischen Kurven. Mit diesen Alternativen kann man die Performance verbessern.
Dieses Verfahren ist allerdings nur zur Vereinbarung eines Schlüssels zwischen zwei Teilnehmern geeignet.

Es wurden verschiedene Versuche unternommen, das DH-Verfahren auf drei oder mehr Teilnehmer zu erweitern (Gruppen DH). Einen Überblick über den Stand der Technik bietet M. Steiner, G. Tsudik, M. Waidner in Diffie-Hellmann Key Distribution Extened to Group Communication, Proc. 3rd ACM Conference on Computer and Communications Security, März 1996, Neu Delhi, Indien.

Eine Erweiterung des DH-Verfahrens auf Teilnehmer A, B und C wird z. B. durch nachfolgende Tabelle beschrieben (Berechnung jeweils mod p):

Teilnehmer A;B;C	A→B	B→C	C→A
1. Runde	g^a	g^b	g^c
2. Runde	g^{ca}	g^{ab}	g^{bc}

Nach Durchführung dieser beiden Runden kann jeder der Teilnehmer den geheimen Schlüssel g^{abc} mod p berechnen.

Weiterhin ist eine Lösung aus Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT´94, Springer LNCS, Berlin 1994 bekannt, bei der zwei Runden zur Generierung des Schlüssels benötigt werden, wobei in der zweiten Runde für n Teilnehmer n Nachrichten der Länge p = ca. 1000Bit gesendet werden müssen.

Weitere relevante Lösungen sind aus M. Burmester and Y. Desmedt, Efficient and secure conference key distribution, Cambridge Workshop on Security Protocols, Springer LNCS 1189, pp 119-129 (1996) bekannt. Hier wird aber vorausgesetzt, daß sichere Kanäle zwischen den Teilnehmern bereits existieren.

Bei allen diesen Erweiterungen tritt mindestens eines der folgenden Probleme auf:

- Die Teilnehmer müssen in einer bestimmten Art und Weise geordnet sein, im obigen Beispiel z. B. als Kreis, d.h. eine Struktur der Teilnehmergruppe muß vorher bekannt sein.
- Wird eine zentrale Stelle zur Koordinierung der Schlüsselvereinbarung verwendet, so haben die Teilnehmer gegenüber dieser Zentrale keinen Einfluß auf die Auswahl des Schlüssels.
- Die Rundenzahl ist abhängig von der Teilnehmerzahl.

Diese Verfahren sind aus den o. g. Gründen in der Regel schwer zu implementieren und sehr rechenaufwendig.

Die Weiterbildung des DH-Verfahrens zu einem Public-Key-Verfahren ist aus T. ElGamal „A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.“, IEEE Transactions on Information Theory, Juli 1985 bekannt.

Das erfindungsgemäße Verfahren muß zur Erzeugung eines gemeinsamen Schlüssels innerhalb einer Gruppe von mindestens drei Teilnehmern geeignet sein. Das Verfahren soll so ausgebildet sein, daß es sich gegenüber den bekannten Verfahren durch geringen Rechenaufwand und geringen Kommunikationsbedarf (wenige Runden auch bei vielen Teilnehmern) auszeichnet. Es soll dabei jedoch einen vergleichbaren Sicherheitsstandard wie das DH-Verfahren aufweisen. Das Verfahren muß einfach zu implementieren sein. Informationen über die Struktur der Gruppe sollen für die Durchführung des Verfahrens nicht benötigt werden.

Das erfindungsgemäße Verfahren, das dieser Aufgabenstellung gerecht wird, basiert auf den gleichen mathematischen Strukturen wie das DH-Verfahren und weist daher vergleichbare Sicherheitsmerkmale auf. Im Vergleich zu den bisher vorgeschlagenen Gruppen-DH-Verfahren ist es jedoch wesentlich effizienter im Hinblick auf Rechenaufwand und Kommunikationsbedarf.

Nachfolgend wird das Wirkprinzip des Verfahrens näher erläutert. Die definierten Teilnehmer am Verfahren werden mit T1-Tn und jeder einzelne nicht konkret benannte Teilnehmer mit Ti bezeichnet. Mit Tj werden alle anderen am Verfahren beteiligten Teilnehmer, ausschließlich des jeweiligen Teilnehmers Ti, bezeichnet. Die öffentlich bekannten Komponenten des Verfahrens sind eine öffentlich bekannte mathematische Gruppe G, vorzugsweise die multiplikative Gruppe aller ganzen Zahlen modulo einer großen Primzahl p und ein Element g der Gruppe G, vorzugsweise eine Zahl $0 < g < p$ mit großer multiplikativer Ordnung. Für die Gruppe G können jedoch auch andere geeignete mathematische Strukturen verwendet werden, z. B. die multiplikative Gruppe eines endlichen Körpers oder die Gruppe der Punkte einer elliptischen Kurve. Das Verfahren wird im Folgenden anhand der Gruppe der Zahlen modulo einer Primzahl p beschrieben.

Dem Verfahren liegen vier Verfahrensschritte zugrunde.
Im ersten Verfahrensschritt wird von jedem einzelnen, nicht konkret benannten Teilnehmer Ti eine Nachricht der Form $Ni = g^{zi} \bmod p$ erzeugt und an alle anderen Teilnehmer Tj gesendet, wobei zi vorzugsweise eine mittels eines Zufallsgenerators gewählte zufällige Zahl aus der Menge $\{1, \ldots p-2\}$ ist.

Im zweiten Verfahrensschritt berechnet jeder Teilnehmer Ti für jeden weiteren Teilnehmer Tj mit $i \neq j$ aus der empfangenen Nachricht g^{zj} einen gemeinsamen Übertragungsschlüssel $k^{ij} := (g^{zj})^{zi}$. Da $k^{ij} = k^{ji}$ gilt, kennen die Teilnehmer Ti und Tj jetzt einen gemeinsamen Übertragungsschlüssel k^{ij} und können daher vertraulich kommunizieren.

Im dritten Verfahrensschritt verwendet jederTeilnehmer Ti den Übertragungsschlüssel k^{ij}, um seine Zufallszahl zi vertraulich an die jeweils anderenTeilnehmer Tj zu übertragen. Die Verschlüsselung der Zufallszahl zi mit dem Übertragungsschlüssel k^{ij} erfolgt dabei mittels eines symmetrischen Verschlüsselungsverfahren. Das bedeutet, daß nach Abschluß des Verfahrensschrittes jeder Teilnehmer Ti außer seiner eigenen Zufallszahl auch die verschlüsselten Zufallszahlen aller anderen Teilnehmer Tj kennt, so daß die Voraussetzungen gegeben sind, einen gemeinsamen Schlüssel k zu berechnen.

Im vierten Verfahrensschritt wird bei jedem Teilnehmer Ti der gemeinsame Schlüssel k nach der Beziehung

$$k = f(z1, z2, ..., zn)$$

berechnet, wobei f eine beliebige symmetrische Funktion ist. Symmetrie bedeutet in diesem Fall, daß der Wert der Funktion, auch bei beliebiger Vertauschung der Argumente, der gleiche bleibt. Beispiele für symmetrische Funktionen sind

- Die Multiplikation in einem (endlichen) Körper: $k := z1 \cdot ... \cdot zn$,
- die Addition in einer (endlichen) Gruppe: $k := z1 + ... + zn$,
- das bitweise XOR der zi: $k := z1 \oplus ... \oplus zn$,
- die Potenzierung von g mit den zi: $k := g^{z1 \cdot ... \cdot zn}$
- zahllose weitere Möglichkeiten.

Das Versenden der in Schritt 1 und 2 generierten Nachrichten kann sowohl über Punkt-zu-Punkt-Verbindungen als auch durch Broadcast oder Multicast durchgeführt werden.

Nachfolgend wird das erfindungsgemäße Verfahren anhand eines konkreten Beispiels für drei Teilnehmer A, B und C näher erläutert. Die Anzahl der Teilnehmer ist jedoch auf beliebig viele Teilnehmer erweiterbar.

Bei diesem Beispiel beträgt die Länge der Zahl p 1024 Bit; g hat eine multiplikative Ordnung von mindestens 2^{160}.

Das erfindungsgemäße Verfahren läuft nach folgenden Verfahrensschritten ab:

1. Teilnehmer A sendet $Na = g^{za} \bmod p$ an die Teilnehmer B und C, Teilnehmer B sendet $Nb = g^{zb} \bmod p$ an die Teilnehmer A und C und Teilnehmer C sendet $Nc = g^{zc} \bmod p$ an die Teilnehmer A und B.
2. Teilnehmer A berechnet $kab = Nb^{za} \bmod p$ und $kac = Nc^{za} \bmod p$. Teilnehmer B und C verfahren analog.
3. Teilnehmer A sendet die Nachricht Mab = E(kab, za) an Teilnehmer B und die Nachricht Mac = E(kac, za) an Teilnehmer C. Hier bezeichnet E(k, m) die symmetrische Verschlüsselung des Datensatzes m mit dem Algorithmus E unter dem Übertragungsschlüssel k^{ij}. Teilnehmer B und C verfahren analog.
4. Teilnehmer A berechnet den gemeinsamen Schlüssel k nach der Funktion $k = g^{ka \bullet kb \bullet kc}$. Analog berechnen die Teilnehmer B und C den gemeinsamen Schlüssel k.

Das oben beschriebene Verfahren kommt mit der minimalen Anzahl von zwei Runden zwischen den Teilnehmern A, B und C aus. Die Anzahl der für die Durchführung des erfindungsgemäßen Verfahrens notwendigen Runden bleibt auch bei einer beliebigen Anzahl von Teilnehmern T1-Tn auf zwei Runden beschränkt.

Eine Variante des Verfahrens besteht darin, vorab einem der Teilnehmer T1-Tn für die Durchführung des zweiten Verfahrensschrittes eine besondere Rolle zuzuweisen. Wird diese Rolle beispielsweise dem Teilnehmer T1 zugeordnet, so werden die Verfahrensschritte 2 und 3 bzw. b und c nur noch von Teilnehmer T1 ausgeführt. Im vierten Verfahrensschritt d berechnen alle am Verfahren beteiligten Teilnehmer T1 – Tn den gemeinsame Schlüssel k nach der Beziehung $k: = h(z1, g^{z2}, ..., g^{zn})$, wobei (x1, x2, ..., xn) eine Funktion sein muß, die in den Argumenten x2, ... xn symmetrisch ist. Diese Variante vermindert die Anzahl der zu sendenden Nachrichten drastisch. Ein Beispiel für eine solche Funktion g ist z. B.

$$k: = h(z1, g^{z2}, ..., g^{zn}) = g^{z1 \bullet z1} \cdot g^{z2 \bullet z1} \cdot ... \cdot g^{zn \bullet z1}.$$

Das erfindungsgemäße Verfahren läßt sich vorteilhaft zur Erzeugung eines kryptografischen Schlüssels für eine Gruppe von mehreren, mindestens jedoch drei Teilnehmern einsetzen.

Aufstellung der Bezugszeichen

T1 – Tn	Teilnehmer 1 bis n
Ti	unbestimmter Teilnehmer von T1-Tn
Tj	unbestimmter Teilnehmer von T1-Tn, verschieden von Ti.
N	Nachricht
Ni	Nachricht eines unbestimmten Teilnehmers Ti
Mab	Nachricht von Teilnehmer A an Teilnehmer B
G	öffentlich bekannte mathematische Gruppe
g	Element der Gruppe G
p	große Primzahl
z	mittels eines Zufallsgenerators gewählte Zufallszahl aus der Menge (1,....p-2)
k^{ij} ; k^{lj}	gemeinsamer Übertragungsschlüssel
k	gemeinsamer Schlüssel
E(,)	Algorithmus
m	Datensatz
f(x1,x2,...,xn)	Funktion symmetrisch in x1,x2,...,xn.
h(x1,x2,...,xn)	Funktion symmetrisch in den Argumenten x2,...,xn.
A; B; C	Benennung der Teilnehmer im Ausführungsbeispiel

Verfahren zum Etablieren eines gemeinsamen Schlüssels für eine Gruppe von mindestens drei Teilnehmern

(2) Patentansprüche

1. Verfahren zum Etablieren eines gemeinsamen Schlüssels für eine Gruppe von mindestens drei Teilnehmern unter Verwendung einer öffentlich bekannten mathematischen Gruppe G und einem öffentlich bekannten Element der Gruppe $g \in G$ von großer Ordnung ,
dadurch gekennzeichnet, daß

a) jeder Teilnehmer (Ti) aus dem öffentlich bekannten Element (g) der Gruppe (G) und einer von ihm gewählten bzw. erzeugten Zufallszahl (zi) eine Nachricht $Ni = (g^{zi} \bmod p)$ erzeugt und an alle anderen Teilnehmer (Tj) sendet, daß

b) jeder Teilnehmer (Ti) aus den von den anderen Teilnehmern (Tj, $j \neq i$) empfangenen Nachrichten (Nj) und seiner Zufallszahl (zi) nach der Funktion $k^{ij} := Nj^{zi} = (g^{zj})^{zi}$ einen Übertragungsschlüssel (k^{ij}) erzeugt, den wegen der Beziehung $k^{ij} = k^{ji}$ auch der Teilnehmer (Tj) kennt, daß

c) jeder Teilnehmer (Ti) an jeden anderen Teilnehmer (Tj) seine Zufallszahl (zi) verschlüsselt schickt, indem er die Nachricht (Mij) gemäß $Mij := E(k^{ij}, zi)$ bildet, wobei $E(k^{ij}, zi)$ ein symmetrischer Verschlüsselungsalgorithmus ist, bei dem der Datensatz (zi) mit dem **gemeinsamen Übertragungsschlüssel (k^{ij})** verschlüsselt wird, und daß

d) jeder Teilnehmer (Ti) den zu etablierenden gemeinsamen Schlüssel (k) aus seiner eigenen Zufallszahl (zi) und den von den anderen Teilnehmern erhaltenen Zufallszahlen (zj), $j \neq i$, nach der Beziehung

$$k := f(z1, ..., zn)$$

ermittelt, wobei f eine symmetrische Funktion sein muß, die invariant unter der Permutation ihrer Argumente ist.

2. Verfahren zum Etablieren eines gemeinsamen Schlüssels nach Anspruch 1, dadurch gekennzeichnet, daß

a) alle am Verfahren beteiligten Teilnehmer (Ti) die von ihnen erzeugte Nachricht ($Ni = g^{zi}$) an einen vorab für die Durchführung des nachfolgenden Verfahrensschrittes bestimmten Teilnehmer, wie beispielsweise den ersten Teilnehmer (T1), übertragen, daß

b) der erste Teilnehmer (T1) die empfangenen Nachrichten (Nj) der anderen Teilnehmer (Tj, $j \neq 1$) für jeden Teilnehmer (Tj) einzeln mit seiner Zufallszahl (z1) zu jeweils einem Übertragungsschlüssel (k^{1j}) verschlüsselt, den wegen der Beziehung $k^{1j} = k^{j1}$ auch der Teilnehmer (Tj) kennt, daß

c) der erste Teilnehmer (T1) an jeden anderen Teilnehmer (Tj) seine Zufallszahl (z1) verschlüsselt schickt, indem er die Nachricht (M1j) gemäß $M1j := E(k^{1j}, z1)$ bildet, wobei $E(k^{1j}, z1)$ ein symmetrischer Verschlüsselungsalgorithmus ist, bei dem der Datensatz (z1) mit dem gemeinsamen Übertragungsschlüssel (k^{1j}) verschlüsselt wird, und daß

d) jeder Teilnehmer (Ti) den zu etablierenden gemeinsamen Schlüssel (k) aus den Werten (Ni) und (Nj), $j \neq i$ und der vom ersten Teilnehmer (T1) verschlüsselt übertragenen Zufallszahl (z1) mit Hilfe der Formel

$$k := h(z1, g^{z2}, ..., g^{zn}),$$

ermittelt, wobei h (x1, x2, ..., xn) eine in den Argumenten x2, ..., xn symmetrische Funktion ist.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 00/06510

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	LENNON R E ET AL: "Cryptographic key distribution using composite keys" BIRMINGHAM,ALABAMA, DEC.3-6, 1978,NEW YORK, I.E.E.E,US, vol. CONF. 1978, 3 December 1978 (1978-12-03), pages 26101-26116-6, XP002098158 page 26.1.4, left-hand column, line 23 -page 26.1.5, right-hand column, line 8 page 26.1.6, left-hand column, line 14 - line 17	1
Y	MENEZES ET AL.: "HANDBOOK OF APPLIED CRYPTOGRAPHY" 1997 , CRC PRESS , BOCA RATON (US) XP002152150 page 528, line 22 - line 24	1

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 November 2000	22/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 00/06510

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7 April 1993 (1993-04-07) page 9, line 10 - line 23	1
A	BURMESTER M ET AL: "SECURE AND EFFICIENT CONFERENCE KEY DISTRIBUTION SYSTEM" ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES,SPRINGER VERLAG,DE, 1995, pages 275-286, XP000934269 cited in the application page 279, paragraph 3.3	1

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 00/06510

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0535863 A	07-04-1993	US 5241599 A	31-08-1993
		AU 648433 B	21-04-1994
		AU 2351392 A	08-04-1993
		CA 2076252 A,C	03-04-1993
		JP 2599871 B	16-04-1997
		JP 6169306 A	14-06-1994
		NO 923740 A	05-04-1993

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/06510

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, INSPEC, PAJ, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	LENNON R E ET AL: "Cryptographic key distribution using composite keys" BIRMINGHAM,ALABAMA, DEC.3-6, 1978,NEW YORK, I.E.E.E,US, Bd. CONF. 1978, 3. Dezember 1978 (1978-12-03), Seiten 26101-26116-6, XP002098158 Seite 26.1.4, linke Spalte, Zeile 23 -Seite 26.1.5, rechte Spalte, Zeile 8 Seite 26.1.6, linke Spalte, Zeile 14 - Zeile 17	1
Y	MENEZES ET AL.: "HANDBOOK OF APPLIED CRYPTOGRAPHY" 1997 , CRC PRESS , BOCA RATON (US) XP002152150 Seite 528, Zeile 22 - Zeile 24	1

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
7. November 2000	22/11/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/06510

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7. April 1993 (1993-04-07) Seite 9, Zeile 10 - Zeile 23	1
A	BURMESTER M ET AL: "SECURE AND EFFICIENT CONFERENCE KEY DISTRIBUTION SYSTEM" ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES,SPRINGER VERLAG,DE, 1995, Seiten 275-286, XP000934269 in der Anmeldung erwähnt Seite 279, Absatz 3.3	1

2

INTERNATIONALER [redacted]HERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

[redacted]tionales Aktenzeichen
PCT/EP 00/06510

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0535863 A	07-04-1993	US 5241599 A	31-08-1993
		AU 648433 B	21-04-1994
		AU 2351392 A	08-04-1993
		CA 2076252 A,C	03-04-1993
		JP 2599871 B	16-04-1997
		JP 6169306 A	14-06-1994
		NO 923740 A	05-04-1993